



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/678,689	10/03/2000	Graham Arthur Makinson	NAIIP161/00.113.01	6810

28875 7590 06/04/2004

SILICON VALLEY INTELLECTUAL PROPERTY GROUP  
P.O. BOX 721120  
SAN JOSE, CA 95172-1120

EXAMINER

OSMAN, AHMED A

ART UNIT	PAPER NUMBER
----------	--------------

2136

DATE MAILED: 06/04/2004

7

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/678,689

Applicant(s)

MAKINSON ET AL.

Examiner

Ahmed A Osman

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 24 October 2003.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-63 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-63 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date 6.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_.

## **DETAILED OFFICE ACTION**

1. Claims 1-63 are presented for examinations.

### ***Claim Objections***

2. Claims 14, 35, and 56 are objected to because of the following informalities:

On page 14, line 19, the phrase "program module provides does not" should apparently be replaced with – program module does not --.

On page 17, line 23, the phrase "program module provides does not" should apparently be replaced with – program module does not --.

On page 20, line 29, the phrase "program module provides does not" should apparently be replaced with – program module does not --.

Appropriate correction is required.

### ***Claim Rejections - 35 USC § 112***

3. Claims 12, 33, and 54 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 12 is dependent on Claim 11, 10, and 1. Claim 12 refers to a said module signature data as being associated with a said anti-virus computer program module.

The applicant fails to associate the module signature data with the anti-virus program

module at any point prior to this claim. Moreover, the applicant claims that the module signature data is the said core signature data. This claim conflicts with the applicant's claim in Claim 1.

Claim 33 is dependent on Claim 32, 31, and 22. Claim 33 refers to a said module signature data as being associated with a said anti-virus computer program module. The applicant fails to associate the module signature data with the anti-virus program module at any point prior to this claim. Moreover, the applicant claims that the module signature data is the said core signature data. This claim conflicts with the applicant's claim in Claim 22.

Claim 54 is dependent on Claim 53, 52, and 43. Claim 54 refers to a said module signature data as being associated with a said anti-virus computer program module. The applicant fails to associate the module signature data with the anti-virus program module at any point prior to this claim. Moreover, the applicant claims that the module signature data is the said core signature data. This claim conflicts with the applicant's claim in Claim 43.

### ***Claim Rejections - 35 USC § 102***

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1, 3, 21, 22, 24, 42, 43, 45, and 63 are rejected under 35 U.S.C. 102(b) as being clearly anticipated by US Patent No. 5,724,425 to Chang.

Chang teaches a method and apparatus utilizing public key encryption techniques for enhancing software security and for distributing software (Column 3 Line 15). Chang further teaches that the present invention may be implemented in software executed by computer (Column 6 Line 17).

As per claims 1, 22, and 43:

**“Reading module signature data associated with said additional computer program module”**

Chang teaches a step where the computing platform determines if the software passport includes an application writer's license, and if it does, the hardware platform extracts the application writer's license from the passport and determines whether or not the passport includes the platform builder's signature. The signature is then decrypted using the public key provided in the platform (Column 4 Line 17).

**“Reading core signature data and other signature data associated with said core computer program”**

**“Comparing said module signature data with said core signature data and said other signature data”**

Chang teaches a step where the computing platform recomputes the message digest of the application writer's license and compares the received message digest with the recomputed message digest (Column 4 Line 25). Chang further teaches that if the digests are equal then the hardware platform extracts the application writer's public key from the application writer's license and extracts the application writer's digital signature (Column 4 Line 29). Chang continues on and states that the hardware platform recomputes the message digest of the binary code comprising the application to be executed and decrypts the application writer's digital signature using the application writer's public key, and then compares the recomputed message digest for the binary code with the application writer's decrypted signature (Column 4 Line 32).

**“Refusing authorization of said additional computer program module for use with said core computer program unless said module signature data matches at least one of said core signature data said other signature data”**

Chang teaches that if the recomputed message digest and received message digest are not equal, then the software passport is not genuine and is rejected (Column 4 Line 27). Chang further teaches that if the recomputed message digest for the binary

code and the application writer's decrypted signature are equal then the binary code is executed by the platform (Column 4 Line 39).

As per claims 3, 24, and 45:

**“Wherein said addition computer program module is refused authorization for use with said core computer program unless said module signature matches both of said core signature data and said other signature data”**

Chang teaches that if the recomputed message digest and received message digest are not equal, then the software passport is not genuine and is rejected (Column 4 Line 27). Chang further teaches that if the recomputed message digest for the binary code and the application writer's decrypted signature are equal then the binary code is executed by the platform (Column 4 Line 39).

As per claims 21, 42, and 63:

**“Writing said additional computer program module”**

Chang teaches a set of application writers who are authorized to write application code for a particular platform (Column 8 Line 67). Chang further teaches a software produced by a licensed application writer.

**“Providing said additional computer program module to a new user”**

Chang teaches that the software passport is then distributed to a user using any number of software distribution models known in the industry (Column 3 Line 35).

**“Said new user associating user signature data with said additional computer program module”**

Chang teaches that the digital signature of the application writer is produced and embedded in the passport.

**“Providing said additional computer program module and associated user signature data to a provider of said core computer program”**

Chang teaches a first computer which is provided with source code to be protected. In addition the first computer is provided with the software application writer's private key along with an application writer's license (Column 3 Line 18). The application writer's license includes identifying information such as the application writer's name as well as the application writer's public key (Column 3 Line 23).

**“Said provider of said core computer program associating core signature data with said additional computer program module and associated user signature data”**

Chang teaches that the first computer encrypts the message digest using the application writer's private key such that the encrypted message digest is defined as a digital signature of the application writer (Column 3 Line 29).



**“Providing said additional computer program module and associated user signature data and core signature data to said new user”**

Chang teaches that the software passport is then distributed to a user using any number of software distribution models known in the industry (Column 3 Line 35).

6. Claims 1, 4, 22, 25, 43, and 46 are rejected under 35 U.S.C. 102(b) as being clearly anticipated by US Patent No. 5,311,591 to Fischer.

Fischer teaches a method and apparatus for providing digital information with enhanced security and protection (Column 1 Line 16).

As per claims 1, 22, and 43:

**“Reading module signature data associated with said additional computer program module”**

**“Reading core signature data and other signature data associated with said core computer program”**

**“Comparing said module signature data with said core signature data and said other signature data”**

**“Refusing authorization of said additional computer program module for use with said core computer program unless said module signature data matches at least one of said core signature data said other signature data”**

Fischer teaches an apparatus that utilizes a unique operating system design that includes a system monitor which limits the ability of a program about to be executed to the use of predefined resources (Column 2 Line 13). Fischer further teaches that the programs about to be executed are digitally signed by some entity that the user trusts and that signature is verified to ensure that the program is trusted and has not been tampered with (Column 2 Line 54). Fischer additionally states that if block 306 indicates that there is a digital signature from the manufacturer in block 308, then the manufacturer's pedigree will be verified by verifying the digital signature and performing whatever certification and authorization checks are appropriate (Column 16 Line 24). Fischer further states that if the signatures are not determined to be valid, then the routine branches to block 324 where the execution in program X is suppressed (Column 16 Line 64).

As per claims 4, 25, and 46:

**“Wherein said module signature data, said core signature data, and said other signature data include public key infrastructure signatures”**

Fischer teaches that the authorization signature includes a signature segment which may include a reference to the signer's certificate which contains the user's public key and name (Column 6 Line 23). Therefore it is determined that the signature data includes public key infrastructure signatures.

7. Claims 1, 2, 5-7, 16, 22, 23, 26-28, 37, 43, 44, 47-49, and 58 are rejected under 35 U.S.C. 102(e) as being clearly anticipated by US Patent No. 6,151,643 to Cheng.

Cheng teaches a method and system that automatically updates software components from numerous vendors on the computer systems of a plurality of end users (Column 2 Line 63). Cheng further teaches a computer-implemented method of providing information for software residing on a client computer (Column 25 Line 35).

As per claims 1, 22, and 43:

**“Reading module signature data associated with said additional computer program module”**

**“Reading core signature data and other signature data associated with said core computer program”**

**“Comparing said module signature data with said core signature data and said other signature data”**

**“Refusing authorization of said additional computer program module for use with said core computer program unless said module signature data matches at least one of said core signature data said other signature data”**

Cheng teaches a method that automatically updates software components from numerous vendors on the computer systems of a plurality of end users (Column 2 Line 63). Cheng further teaches a step 203 where the registered users are authenticated by the service provider computer 102 using conventional authentication mechanisms such

as digital signatures, certificates, or the like. Authentication ensures that only registered users who are properly authorized by the service provider can obtain software updates (Column 7 Line 40). Authentication of the software updates ensures that the software updates are virus free and uncorrupted (Abstract Line 26). Cheng teaches a security module 701 which handles the authentication of the users which may be implemented with conventional authentication mechanisms based on digital signatures, such as public key systems supporting digital signatures, certificates and the like (Column 16 Line 39). Cheng additionally teaches that the security module 701 provides for verification of the integrity of software updates that are downloaded from the software vendor to ensure that such updates have not been altered or infected by computer viruses or other modifications (Column 16 Line 48).

As per claims 2, 23, and 44:

**“Wherein said other signature data is user signature data”**

Cheng teaches a registration process 202 that assigns users a unique registration number and that number is stored on the client computer to be used during subsequent logins to identify the user to the service provider computer (Column 7 Line 35).

As per claims 5, 26, and 47:

**“Wherein said other signature data is associated with said core computer program upon installation of said core computer program”**

Cheng teaches a registration process 202 that assigns users a unique registration number and that number is stored on the client computer to be used during subsequent logins to identify the user to the service provider computer (Column 7 Line 35).

As per claims 6, 27, and 48:

**“Wherein said other signature data is embedded within said core computer program”**

Cheng teaches a registration process 202 that assigns users a unique registration number and that number is stored on the client computer to be used during subsequent logins to identify the user to the service provider computer (Column 7 Line 35).

As per claims 7, 28, and 49:

**“Wherein said user signature data is embedded within said core computer program by applying a user specific patch to said core computer program”**

Cheng teaches a registration process 202 that assigns users a unique registration number and that number is stored on the client computer to be used during subsequent logins to identify the user to the service provider computer (Column 7 Line 35).

As per claims 16, 37, and 58:

**“Wherein said additional computer program module is operable to install another computer program”**

Cheng teaches that client application performs the installation, executing any necessary decompression, installation, or setup applications necessary to install the software update (Column 9 Line 3).

8. Claims 1, 22, and 43 are rejected under 35 U.S.C. 102(e) as being clearly anticipated by US Patent No. 6,157,721 to Shear.

Shear teaches a system and method using cryptography to protect secure computing environments (Column 1 Line 1).

As per claims 1, 22, and 43:

**“Reading module signature data associated with said additional computer program module”**

Shear teaches a method where a protected processing environment can distinguish between authorized and unauthorized load modules by examining the load module to see whether it bears the seal of verifying authority (Column 9 Line 58).

Shear further discloses that the digital sealing process is actually performed by creating a “digital signature” using a well-known process (Column 10 Line 58).

**“Reading core signature data and other signature data associated with said core computer program”**

**“Comparing said module signature data with said core signature data and said other signature data”**

Shear teaches that the protected processing environment compares the version of message digest it obtains from the digital signature with the version of message digest it calculates itself from the load module using the one way hash transformation (Column 14 Line 52).

**“Refusing authorization of said additional computer program module for use with said core computer program unless said module signature data matches at least one of said core signature data said other signature data”**

Shear teaches that the message digests mentioned above should be identical. If they do not match, then digital signature 106 is not authentic or load module 54 has been changed and protected processing environment 108 rejects load module 54 (Column 14 Line 56).

9. Claims 1, 10, 11, 13-15, 17-20, 22, 31, 32, 34-36, 38-41, 43, 52, 53, 55-57, and 59-62 are rejected under 35 U.S.C. 102(e) as being clearly anticipated by US Patent No. 6,108,420 to Larose.

Larose teaches a method and system for the electronic distribution and installation to users via a network (Column 1 Line 7).

As per claims 1, 22, and 43:

**“Reading module signature data associated with said additional computer program module”**

Larose teaches a step where the program examines the file to determine the location of the overall cryptographic signature, the embedded data cryptographic signature and embedded data (Column 12 Line 53).

**“Reading core signature data and other signature data associated with said core computer program”**

Larose teaches a step where a local version of the overall cryptographic signature is calculated using the same known cryptographic signature algorithm that was employed by the SDA 100 (Column 13 Line 1).

**“Comparing said module signature data with said core signature data and said other signature data”**

Larose teaches that the locally calculated overall fingerprint is compared to the decrypted remote overall fingerprint (Column 13 Line 9). Larose further teaches that the locally calculated embedded data fingerprint is compared to the decrypted remote embedded data fingerprint (Column 13 Line 27).



**“Refusing authorization of said additional computer program module for use with said core computer program unless said module signature data matches at least one of said core signature data said other signature data”**

Larose teaches that if either or both of the above mentioned comparison differ, then the authentication and reading program will fail with a warning that the installed aggregate distribution file has been corrupted (Column 13 Lines 11 and 29).

As per claims 10, 31, and 52:

**“Wherein said core computer program is an anti-virus computer program”**

Larose teaches that the authentication and reading program may not be a stand-alone program and could be incorporated as functions of other programs such as a license checker or a virus-checker program (Column 12 Line 24).

As per claims 11, 32, and 53:

**“Wherein said anti-virus computer program operates with at least one updateable anti-virus computer program module”**

Larose teaches that the disclosed method and system can be used to upgrade an installed aggregate distribution file present on an installation computer (Column 14 Line 25).

As per claims 13, 34, and 55:

**“Wherein said additional computer program module provides functionality independent of that of said core computer program”**

Larose teaches that the disclosed method and system can be used to upgrade an installed aggregate distribution file present on an installation computer (Column 14 Line 25).

As per claims 14, 35, and 56:

**“Wherein said additional computer program module provides does not relate to anti-virus protection”**

Larose teaches an example where the disclosed invention could be used in a computer game environment (Column 14 Line 47).

As per claims 15, 36, and 57:

**“Wherein said additional computer program is operable to patch an installed computer program”**

Larose teaches that the disclosed method and system can be used to upgrade an installed aggregate distribution file present on an installation computer (Column 14 Line 25).

As per claims 17, 38, and 59:

**“Writing said additional computer program module”**

Larose teaches a step where an input/output logic 111 of the conversion program 110 reads in the desired original distribution file 130 (Column 7 Line 34). The office concludes that the original file was written at some point in time prior to this step.

**“Receiving new user information from a new user of said additional computer program module”**

Larose teaches a User Installation Agent (UIA) 200 that accepts data 32 input from the user, such as name, address, payment options, etc. (Column 5 Line 21).

**“Generating user signature data specific to said new user in dependence upon said new user information”**

Larose teaches a step 2 which generates a cryptographic signature from the given user information (Column 7 Line 34).

**“Associating said user signature data with said additional computer program module”**

Larose teaches a Secure Distribution Agent (SDA) that combines identifying data, which constitutes information concerning the user, with the data stored in the databases to produce an aggregate distribution file that is uniquely customized, authenticable, and traceable to the user (Column 5 Line 43). Larose further teaches that the output of the conversion program 110 is an aggregate distribution file 170 which contains both the contents of the original distribution file 130, the embedded data 140,

as well as a cryptographic signature of the embedded data an the original distribution file (Column 6 Line 27).

**“Providing said additional computer program module with associated user signature data to said new user”**

Larose teaches embedded data, which can include a unique serial number, used to identify the aggregate distribution file to be distributed to the user. The office concludes that the module is distributed to the user according to the disclosed invention (Column 6 Line 16).

As per claims 18, 39, and 60:

**“Wherein said step of generating uses a tool produced by a provider of said core computer program”**

Larose teaches a conversion program 110 that is used in generating the user signature data. It is clearly illustrated in Figure 2 that the conversion program is part of the SDA.

As per claims 19, 40, and 61:

**“Wherein said step of associating uses a tool produced by a provider of said core computer program”**

Larose teaches a Secure Distribution Agent (SDA) mentioned above that is used in the associating process. Larose teaches that the SDA is resident on a distribution computer that is an essential part of the disclosed invention (Column 4 Line 34).

As per claims 20, 41, and 62:

**“Writing said additional computer program module”**

Larose teaches a step where an input/output logic 111 of the conversion program 110 reads in the desired original distribution file 130 (Column 7 Line 34). The office concludes that the original file was written at some point in time prior to this step.

**“Generating signature data specific to said additional computer program module in dependence upon said additional computer program module using a tool produced by a provider of said core computer program”**

Larose teaches a step 2 which generates a cryptographic signature from the given user information (Column 7 Line 34).

**“Associating said signature data with said additional computer program module”**

Larose teaches a Secure Distribution Agent (SDA) that combines identifying data, which constitutes information concerning the user, with the data stored in the databases to produce an aggregate distribution file that is uniquely customized, authenticable, and traceable to the user (Column 5 Line 43). Larose further teaches

that the output of the conversion program 110 is an aggregate distribution file 170 which contains both the contents of the original distribution file 130, the embedded data 140, as well as a cryptographic signature of the embedded data an the original distribution file (Column 6 Line 27).

**“Providing said additional computer program module with associated signature data to said new user”**

Larose teaches embedded data, which can include a unique serial number, used to identify the aggregate distribution file to be distributed to the user. The office concludes that the module is distributed to the user according to the disclosed invention (Column 6 Line 16).

10. Claims 1, 8, 9, 22, 29, 30, 43, 50, and 51 are rejected under 35 U.S.C. 102(e) as being clearly anticipated by US Patent No. 6,138,236 to Mirov.

Mirov teaches an apparatus for firmware authentication and methods for operating the same which result in software upgradability to firmware (Column 2 Line 7).

As per claims 1, 22, and 43:

**“Reading module signature data associated with said additional computer program module”**

Mirov teaches a computer system 10, which includes a flash PROM 18, which is divided into 2 main sections, an authentication section 45 and a programmable section 55 (Column 3 Line 57). The authentication section authenticates the programmable section to verify that the micro-code instructions are trusted (Column 3 Line 66). The authentication section includes a plurality of secure micro-code 51, a comparator, a hash generator 53, a decryptor 54 and a public key 56 (Column 4 Line 3). The unsecured section 55 includes a digital signature 57 and unsecured micro-code (Column 4 Line 5). Mirov further teaches that during the initialization of the computer system, the secure micro-code of the authentication section executes and directs the hash generator to generate a data hash of the unsecured micro-code programmed in the programmable section (Column 4 Line 8).

**“Reading core signature data and other signature data associated with said core computer program”**

The secure micro-code also directs the decryptor to calculate a verification hash. The decryptor applies the public key of the authentication section and the digital signature and calculates the verification hash (Column 4 Line 12).

**“Comparing said module signature data with said core signature data and said other signature data”**

Mirov teaches that once the verification hash and data hash are generated, the micro-code directs the comparator to compare the verification hash with the data hash.

**“Refusing authorization of said additional computer program module for use with said core computer program unless said module signature data matches at least one of said core signature data said other signature data”**

Mirov teaches that if the verification hash matches the data hash, the unsecured micro-code is properly verified and permitted to execute, and if the comparison of the verification hash and the data hash fails, the unsecured micro-code is corrupted or had been altered without proper authorization (Column 4 Line 21).

As per claims 4, 25, and 46:

**“Wherein said module signature data, said core signature data, and said other signature data include public key infrastructure signatures”**

Mirov teaches that public-key cryptography verifies that the digital signature and the public key decrypts to a verification hash which matches the data hash of the micro-code programmed in the programmable section (Column 4 Line 26). Mirov further teaches that the verification hash is encrypted using public key cryptography techniques (Column 4 Line 61).

As per claims 8, 29, and 50:

**“Wherein said core signature data is associated with said core computer program upon generation of said core computer program”**



Mirov teaches a computer system 10, which includes a flash PROM 18, which is divided into 2 main sections, an authentication section 45 and a programmable section 55 (Column 3 Line 57). The authentication section authenticates the programmable section to verify that the micro-code instructions are trusted (Column 3 Line 66). The authentication section includes a plurality of secure micro-code 51, a comparator, a hash generator 53, a decryptor 54 and a public key 56 (Column 4 Line 3). The unsecured section 55 includes a digital signature 57 and unsecured micro-code (Column 4 Line 5).

As per claims 9, 30, and 51:

**“Wherein said core signature data is embedded within said core computer program”**

Mirov teaches a computer system 10, which includes a flash PROM 18, which is divided into 2 main sections, an authentication section 45 and a programmable section 55 (Column 3 Line 57). The authentication section authenticates the programmable section to verify that the micro-code instructions are trusted (Column 3 Line 66). The authentication section includes a plurality of secure micro-code 51, a comparator, a hash generator 53, a decryptor 54 and a public key 56 (Column 4 Line 3). The unsecured section 55 includes a digital signature 57 and unsecured micro-code (Column 4 Line 5).

### ***Conclusion***

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

The following patents are cited to further show the state of the art with respect to data processing systems in general:

U.S. Patent No. 5,933,503 to Schell et al.

U.S. Patent No. 5,970,145 to McManis

U.S. Patent No. 6,067,575 to McManis et al.

U.S. Patent No. 6,618,855 to Lindholm et al.

U.S. Patent No. 6,651,249 to Waldin et al.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ahmed A Osman whose telephone number is 703-305-8910. The examiner can normally be reached on M-F.

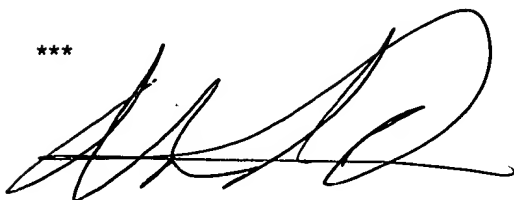
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-305-3718.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Application/Control Number: 09/678,689  
Art Unit: 2136

Page 26

\*\*\*

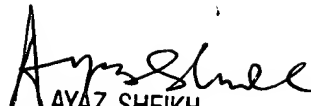


Ahmed Osman

United States Patent & Trademark Office

Patent Examiner – AU 2136

February 18, 2004



AYAZ SHEIKH  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100